Using Digital Manufacturing Certificates for Authorization, Authentication & Traceability of Product Data

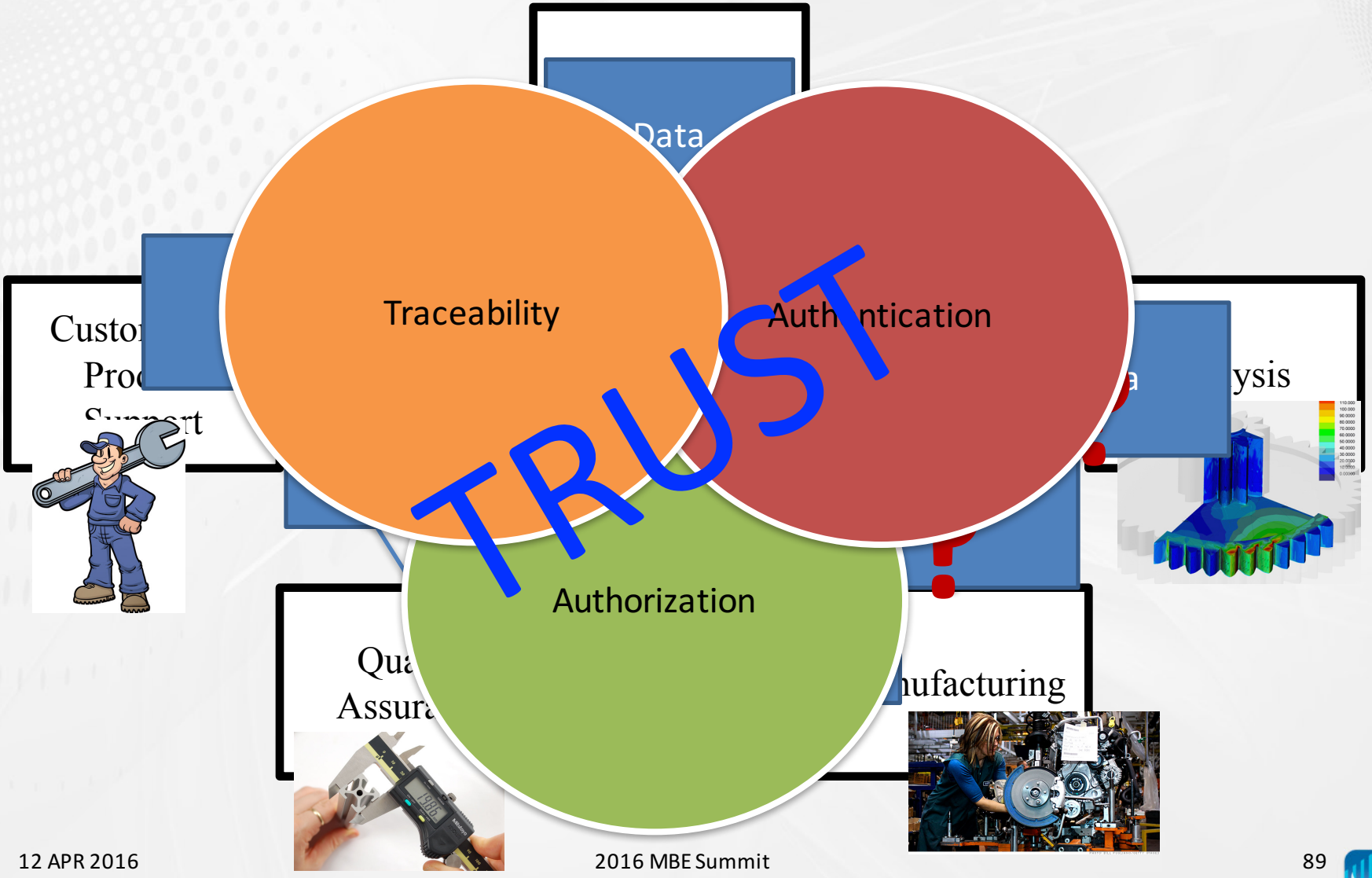
Sylvere Krima

Engisis LLC

with Systems Integration Division

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

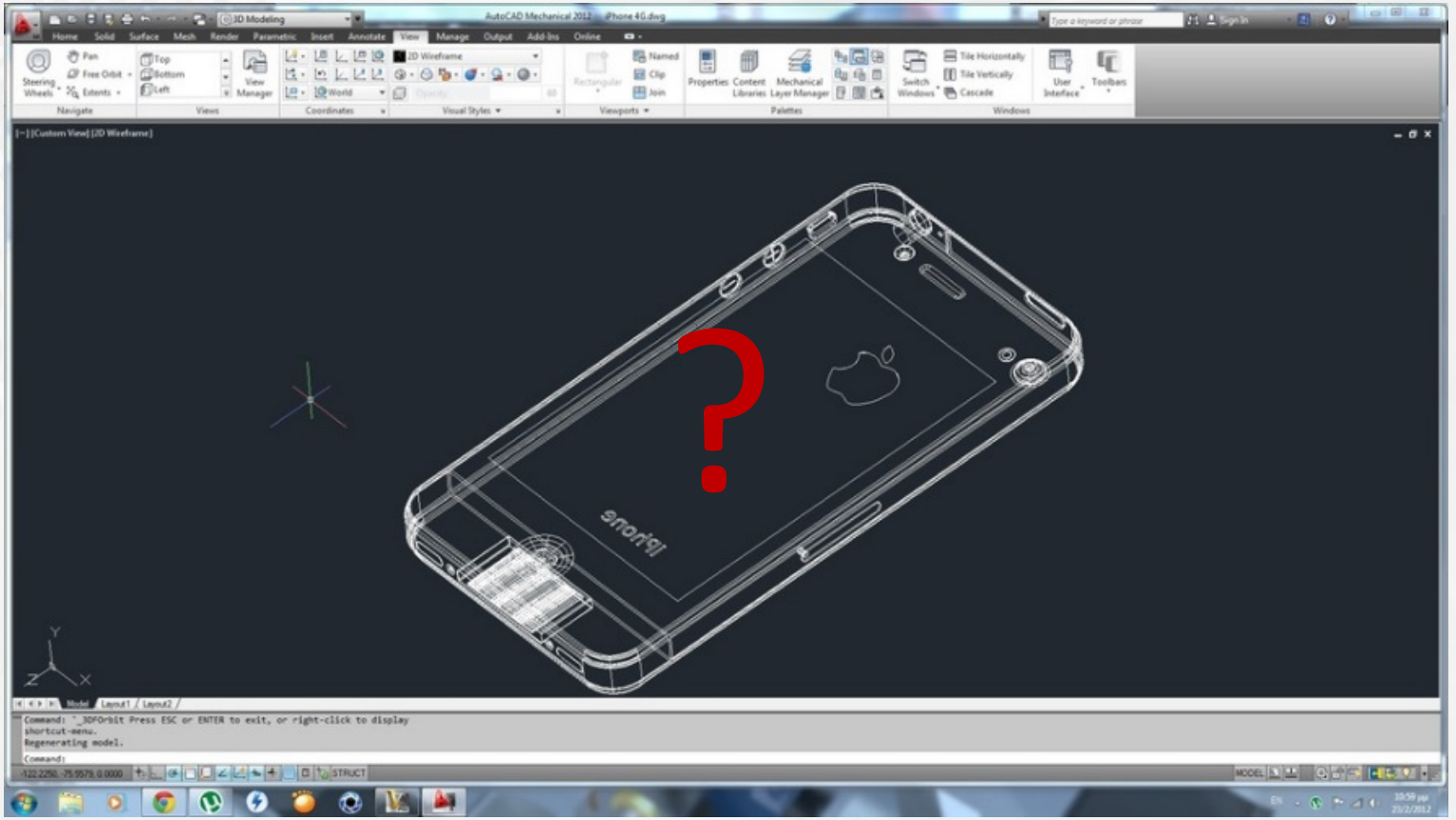
Objective


Data
Traceability
Authentication
TRUST
Authorization
Custo
Proc
Support
ysis
Qua
Assura
nufacturing

Objective

- Authentication: WHO did *what* to whom?
  - Sylvere *acknowledges* that XYZ-123 is his design
- Authorization: WHAT can be done to whom?
  - Tom *approves* Sylvere's design XYZ-123 to be used for production
- Traceability: Where/When was this done?
  - On April 1st, Tom approved XYZ-123 to be used for production

Problem



Requirements

- Reliable (R1)
  - If the data is altered after embedding information, trust is broken!
- Flexible mechanism to embed Trust metadata (R2)
  - Everyone has their own flavor of metadata
- Support standard formats for digital product data (R3)

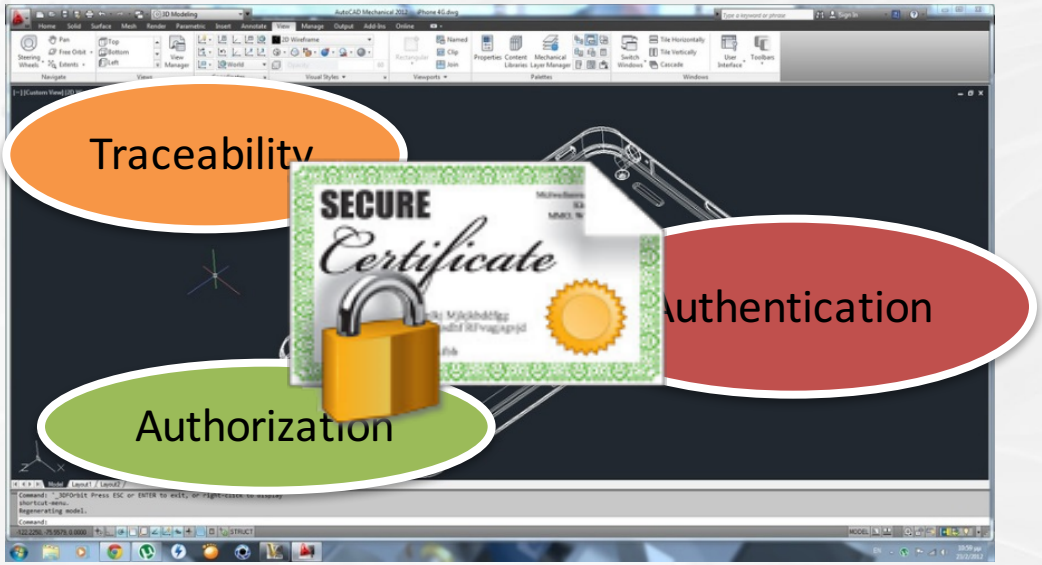
Our approach

- Reliable (R1)
  - Identify when data has been altered
- Leverage X.509 certificates and digital signature mechanism
  - standardized and proven
- Flexible (R2)
  - Cannot support new metadata “on the fly”
- Support from product data standards (R3)
  - Weak

Our approach (2)

- Killed two birds with one ***stone***
  - ***Extended*** product data standards to embed trust metadata (R3)
    - ISO 10303 STEP
    - QIF
  - ***Extensions*** are generic and support infinity of metadata (R2)

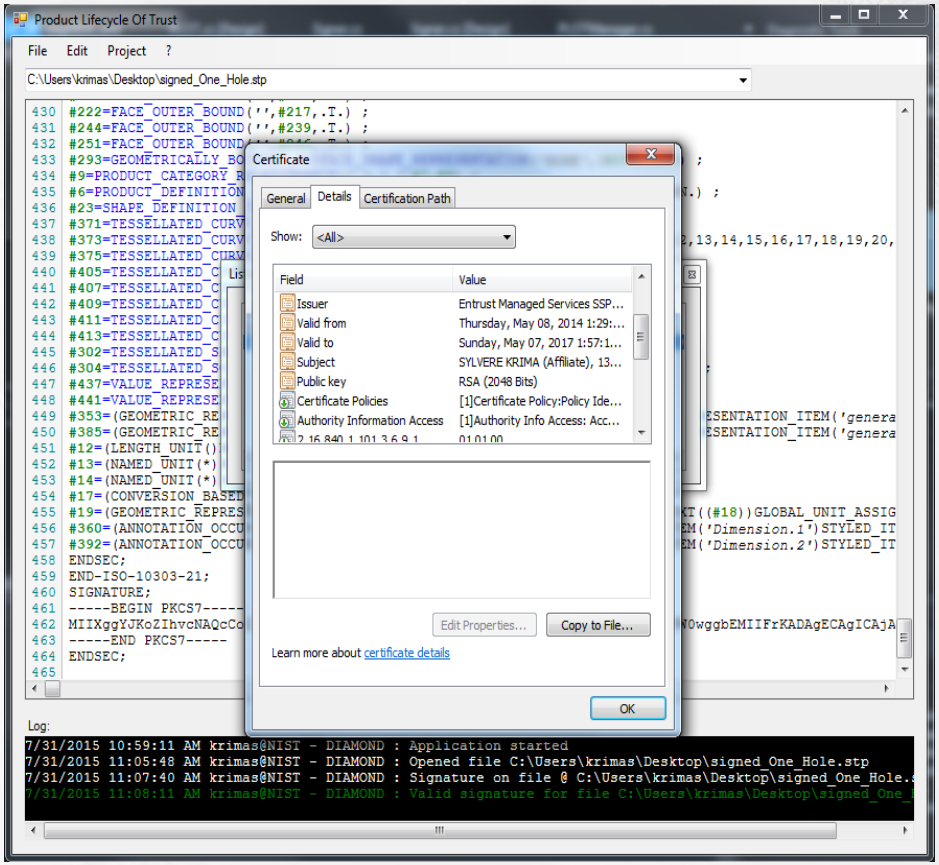
Our approach (3)




```
TRACE:#3421
#3422 = PKCS_TRACE({source:`URI:15.1115\734.13.phone',
       date:`17-FEB-2016', operation:`validation',
       usage:`development', result:`pass with warnings',
       report:`URI:15.1115\734.13.phone.validation'})
#3423 = PKCS(`pkcs7_signature',Y,[#3415,#3418])
ENDSEC;
```

Digital Manufacturing Certificate Toolkit

- Toolkit includes a User Interface and API for Reading, Writing, and Verifying digital signatures in models



- Supports G-Code (ISO 6983), QIF 2.1, PDF/PRC, and STEP P21 formats

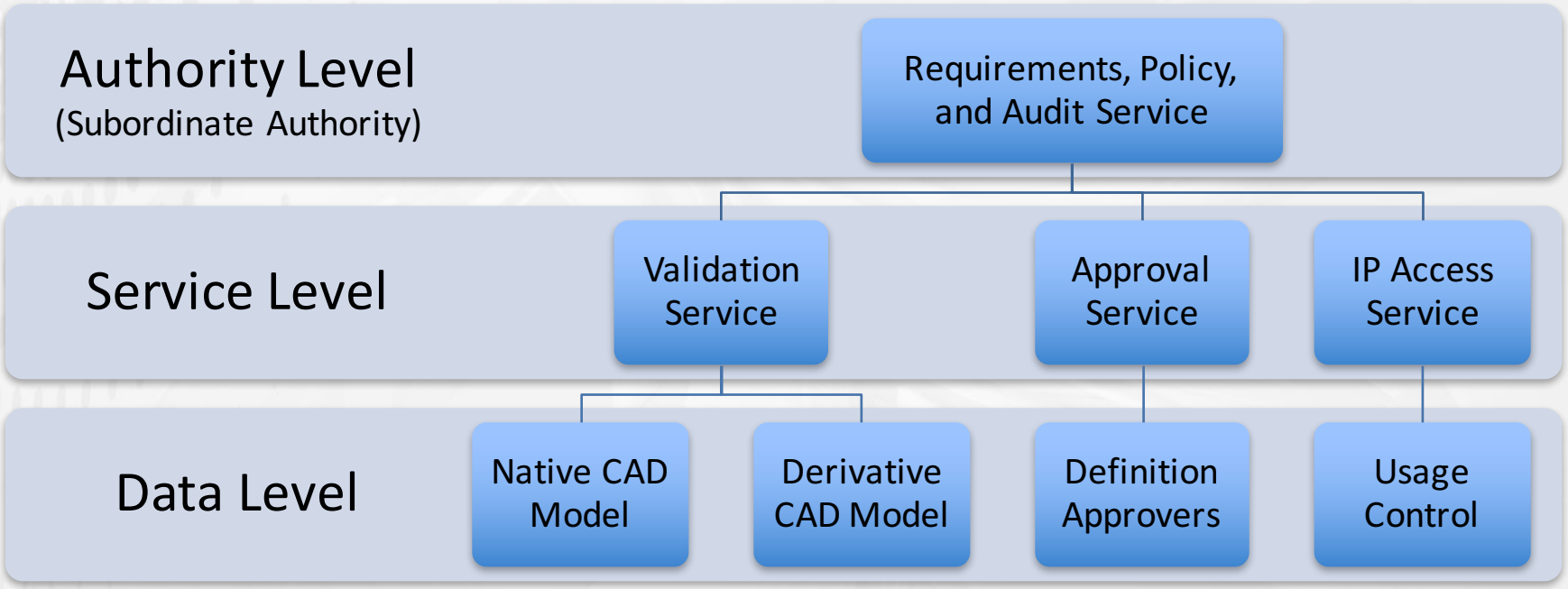
- Toolkit and source code available at: https://github.com/usnistgov/DT4SM

Our contributions

- Extensions to product data standards for embedding trust metadata
- Easy adoption by manufacturers (Toolkit)
- Faster implementation by solution providers (API)

Lastly, Proposing a Product Lifecycle of Trust

A concept inline with X.509 Private Key Infrastructure and Privilege Management Infrastructure as an all-in-one solution



A system based on Authorization with embedded Authentication.

(what the data is) **(how the data can is used)**